

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 3:18-cr-00074-JAG
	)	
JOHN GLENN WEED,	)	
	)	
<i>Defendant.</i>	)	

**GOVERNMENT’S RESPONSE IN OPPOSITION TO DEFENDANT’S  
MOTION FOR A BILL OF PARTICULARS**

The United States of America, by and through its attorneys, G. Zachary Terwilliger, United States Attorney for the Eastern District of Virginia, and Brian R. Hood, Assistant United States Attorney, hereby responds in opposition to the defendant’s Motion for a Bill of Particulars. (Docket No. 21.) For the reasons set forth below, the defendant’s motion should be denied.

**I. INTRODUCTION AND FACTUAL SUMMARY**

As set forth in a search warrant affidavit related to this case<sup>1</sup>, the defendant, JOHN GLENN WEED, was a computer systems architect employed by The Analytic Sciences Corporation (TASC), Chantilly, Virginia, which was a contractor for the National Reconnaissance Office (NRO). While at TASC the defendant developed the Tactical Dissemination Network (TDN), which was a network designed to process and transmit information used by the military and the intelligence community in support of the United States’ war against terrorism. As part of his duties, WEED also worked with radio transmitters commonly referred to as “Blue Force Trackers” (“BFTs”) or “Friendly Force Trackers” (“FFT”). These devices permit operational commanders to track the location of military and

---

<sup>1</sup> Case number 3:13-ms-235, filed August 23, 2013.

intelligence community assets, such as personnel and vehicles, while those assets conduct missions in operational theaters.

WEED was widely regarded by both peers and colleagues as a brilliant computer coder, but also had a widespread reputation for being a difficult employee and someone who behaved as if the rules did not apply to him. Prior to his termination, he was counseled on multiple occasions for security violations.

As part of a periodic reinvestigation (PR) for WEED's security clearance, an adjudications investigator learned that WEED had been arrested for Driving Under the Influence (DUI) in May 2012, which constituted the third known DUI arrest or conviction the defendant had received while working for TASC and the NRO.<sup>2</sup> The defendant did not report that arrest as required to government officials. The background investigator contacted WEED and scheduled an interview regarding the unreported DUI for September 18, 2012. On that day, the defendant contacted the investigator and stated that he would be unable to come in because he was working on "Iran issues." A review of public records revealed that one week before the proposed interview, on September 11, 2012, WEED had pleaded guilty in Fauquier County Circuit Court for a DWI violation, and that on September 18, 2012, the defendant made an appearance in Fauquier General District Court, which investigators believe was a probation violation hearing that flowed from the defendant's September 11 guilty plea.

The background investigator eventually interviewed WEED about the unreported DUI on September 20, 2012. WEED brought to the interview a photograph of the officer who arrested him for the DUI. The photo WEED displayed bore multiple bullet holes. The defendant stated that he got the picture off the Internet and used the picture of the arresting officer for "target

---

<sup>2</sup> The defendant's other DUI/DWI arrests and convictions occurred in the United Kingdom in 2005, which the defendant self-reported, and in Fauquier County, Virginia, on January 30, 2012.

practice.” WEED believed he was unjustly convicted and that he intended to “ruin the life” of the arresting officer for what he did. WEED’s conduct on this day quickly resulted in his being removed from the premises and barred from entering any TASC or NRO property and facilities. The defendant’s security clearance was revoked and his employment officially terminated several weeks later.

Prior to his termination, WEED had been directed on numerous occasions by his superiors to provide all of the source code and information related to the design and function of the TDN. Even though the TDN was government property to which WEED had no ownership rights, WEED evidently resisted providing the requested information by repeatedly stalling or making excuses for not delivering his work product. WEED eventually turned over information related to the TDN when a supervisor told him that he would not be allowed to travel for his job until he had turned over information related to the TDN. This behavior, coupled with several statements by WEED that emerged during a post-termination review of his emails, suggested to investigators that WEED held an inappropriate attitude of individual ownership regarding his government work product.

Particularly concerning to NRO officials was information received from one of WEED’s coworkers, who reported that WEED once stated words to the effect that “if they ever try to get rid of me I could plant back doors to gain remote access to bring down the system.” Unsurprisingly, officials at TASC and NRO were not confident that they knew everything they should or needed to know regarding WEED’s work on the TDN. These concerns prompted a security review of WEED’s computer following his termination.

A forensic investigation of WEED’s computer at the NRO revealed that on four consecutive days from September 17 to September 20, 2012, a remote desktop protocol (RDP)

session had been established from the defendant's workstation in the NRO to an external computer with the IP address of 71.62.115.229. Remote desktop protocol is a proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection. The defendant's workstation was located in an area called a sensitive compartmented information facility ("SCIF"), which is a secure area designed to safely store highly classified information. For security reasons, SCIFs typically are not designed to provide network access to the external Internet. NRO officials considered these RDP sessions highly suspicious because such connections to the external Internet from the SCIF were not authorized by the NRO's security policies and procedures, and moreover during the sessions there was an exchange of over 800 MB data that, because the data was both compressed and encrypted, investigators were unable to determine its contents.

Forensic analysis also revealed that the external computer that connected to WEED's NRO workstation was named "SUNBLOCK-FITPC2." WEED regularly used the nickname "Sunblock" in the signature line of his NRO emails because he considered himself so critical to the NRO's mission that he was a "single point of failure," also referred to as an "SPF," which is the same abbreviation for the "sun protection factor" used to rate the effectiveness of various suntan and sunblock lotions. A public records check revealed that IP address 71.61.115.229 was owned by Comcast, and records obtained from Comcast indicated that on the relevant dates above that IP address was assigned to the residential internet account for WEED's residence.

Based in part on the above information, FBI Special Agent Steve Hall obtained a search warrant for the defendant's residence in Fredericksburg, Virginia, on August 23, 2013, which agents executed on August 27, 2013. During the search, which investigators

conducted 11 months after WEED was escorted from NRO facilities, investigators seized numerous items of United States government property. Agents found one General Dynamics, Model AATR radio in a cardboard box in the defendant's garage. They also found 11 BFT transmitters stored in hard-shelled pelican cases lying in plain view on the floor in the defendant's basement workshop. These are identified in the pending indictment as "two (2) General Dynamics MTX, Version 1.4 transmitters; eight (8) General Dynamics, Trident Version 1.0 transmitters; [and] one (1) Model PGITR transmitter."

Numerous interviews with WEED's coworkers and supervisors at both TASC and the NRO failed to identify anyone who gave WEED permission to take these devices home and keep them as his personal property. These same interviews failed to identify anyone who knew that WEED had taken these devices home, and further did not suggest that either TASC or the NRO had a permissive work culture where people turned a blind eye to others taking home and permanently keeping government property. WEED also signed numerous nondisclosure agreements as part of his employment, all of which contained the provision that all property he obtained during his employment with TASC and the NRO remained government property and was to be returned to the government upon the termination of his employment. These 12 radios, the AATR and the 11 BFTs, thus became the basis for Count One of the defendant's indictment, charging him with theft of government property, in violation of Title 18, United States Code, Section 641.

## **II. LEGAL ANALYSIS**

Under FED.R.CRIM.P. 7(f), the court may direct the filing of a bill of particulars if appropriate. *United States v. Bales*, 813 F.2d 1289, 1294 (4th Cir. 1987). The purpose of a bill of particulars is to "inform the defendant of the charges against him in sufficient detail and to

minimize surprise at trial.” *United States v. Butler*, 885 F.2d 195, 199 (4th Cir. 1989). The function of a bill of particulars is not to provide detailed disclosure of the government’s evidence in advance of trial, but rather to supply any essential detail that may have been omitted from the indictment. *United States v. Anderson*, 481 F.2d 685, 690-91 (4th Cir. 1973). The defendant therefore does not have an unconditional right to such a bill. *Butler*, 885 F.2d at 199.

Where the Government provides the defendant with the information necessary to avoid unfair surprise, either through the indictment or some other means, no bill of particulars is required. *United States v. Gia Le*, 310 F.Supp.2d 763, 781-82 (E.D. Va. 2004) (denying a bill of particulars where the Government has “provided discovery” as to the alleged incident, and the defendants were “receiving additional facts regarding th[e] incident through ongoing discovery.”). In light of its limited purpose, a bill of particulars is not appropriate in order to “provide detailed disclosure of the government’s evidence in advance of trial.” *United States v. Fletcher*, 74 F.3d 49, 53 (4th Cir. 1996). Indeed, when a defendant’s motion for a bill of particulars amounts to such a fishing expedition, the settled law is that such motions must be denied:

[I]t is well-settled that a bill of particulars . . . must “not . . . be used to provide a detailed disclosure of the government’s evidence in advance of trial.” . . . Thus, a court must not direct the government to reveal the details of its evidence or the precise manner in which it will make its proof in a bill of particulars.

*Gia Le*, 310 F.Supp. at 781 (E.D. Va. 2004) (citing *United States v. Automated Medical Labs., Inc.*, 770 F.2d 399, 405 (4th Cir.1985)).

The granting or denial of a bill of particulars is within the court’s discretion. *United States v. Bales*, 813 F.2d 1289, 1294 (4th Cir. 1987). To establish an abuse of discretion, a defendant must prove that he or she suffered unfair surprise. *United States v. Jackson*, 757 F.2d

1486, 1491 (4th Cir. 1985).

In his motion for a bill of particulars, the defendant requests that the Government provide:

- 1 The serial numbers of each item allegedly embezzled.
- 2 The date each item was allegedly embezzled.
- 3 The Government agency that owned each item at the time of the alleged embezzlement.
- 4 The Government authority that signed and handed the items over to the Defendant.
- 5 The purpose the item was handed over to the Defendant.

As to questions 1 and 3, the government has separately provided that information to counsel for defendant since his filing of the defendant's motion for a bill of particulars.

Regarding the remaining items, such questions either assume the existence of facts that the government does not believe exist, or is a request for the "when, where and how" the defendant committed the charged offense that is the equivalent of a request for complete discovery that is routinely denied by courts. *See, e.g., See United States v. Automated Medical Laboratories, Inc.*, 770 F.2d 399, 405 (4th Cir. 1985) ("A bill of particulars is not to be used to provide detailed disclosure of the government's evidence in advance of trial."); *United States v. Giese*, 597 F.2d 1170, 1181 (9th Cir. 1979) ("Appellant's request for the 'when, where, and how' of every act in furtherance of the conspiracy was equivalent to a request for complete discovery of the government's evidence, which is not a purpose of the bill of particulars.").

In his Memorandum in Support of Motion for Bill of Particulars (Docket No. 22), the defendant makes two arguments that are devoid of legal or factual support. The first such argument is that "Count One fails to state any of the alleged overt acts necessary to support the government's charge that embezzlement existed, and John Weed was involved in it." Beyond the

fact that Section 641 does not have as an element the requirement that the government prove an overt act<sup>3</sup>, even if there were such a requirement a defendant would not be entitled to that information through a bill of particulars. *See, e.g., United States v. Rosenthal*, 793 F.2d 1214, 1227 (11th Cir. 1986) (government required to provide defendants with all overt acts that might be proven at trial).

The defendant's memorandum also contains the argument that "... the indictment fails to address the fact that the items were authorized to be in custody of the Defendant for an unknown amount of time, and for an unknown purpose." As explained above, numerous interviews with TASC and NRO personnel revealed no such fact. Furthermore, as explained in the government's Response in Opposition to the Defendant's Motion to Dismiss, there is no such requirement to address the above assertions in an indictment.

### III. CONCLUSION

For all of the above reasons, then, the United States respectfully requests that the Court deny the defendant's Motion for a Bill of Particulars.

Respectfully submitted,

G. ZACHARY TERWILLIGER  
UNITED STATES ATTORNEY

By: /s/ Brian R. Hood  
Assistant United States Attorney  
United States Attorney's Office  
919 East Main Street, Suite 1900  
Richmond, VA 23219  
Telephone: (804) 819-5400  
Email: [brian.hood@usdoj.gov](mailto:brian.hood@usdoj.gov)

---

<sup>3</sup> "To obtain a conviction under 18 U.S.C. § 641, the government must establish beyond a reasonable doubt that: (1) the money or property described in the indictment is money or a thing of value of the United States (2) that the defendant stole, fraudulently received, or converted to his own use (3) with the intent to permanently or temporarily deprive the government of that money or thing of value." *United States v. Kiza*, 855 F.3d 596, 601 (4th Cir. 2017) (citing *United States v. Hamilton*, 699 F.3d 356, 363 (4th Cir. 2012)).



**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that on **September 14, 2018**, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all parties of record.

Respectfully submitted,

G. ZACHARY TERWILLIGER  
UNITED STATES ATTORNEY

By: /s/ Brian R. Hood  
Assistant United States Attorney  
United States Attorney's Office  
919 East Main Street, Suite 1900  
Richmond, VA 23219  
Telephone: (804) 819-5400  
Email: [brian.hood@usdoj.gov](mailto:brian.hood@usdoj.gov)